Certificate Issuing and Management Components (CIMCs) Protection Profile (PP)

August 10, 2000

Annabelle Lee

National Institute of Standards and Technology

PKI Components

- Components of a PKI:
  - Certificate Issuing & Management System (CIMS)
  - Certificate Issuing and Management Components (CIMC)
  - Repository
  - End-Entity/Client
  - Archive
  - Key Recovery

Certificate Issuing and Management System (CIMS)

- Includes components of PKI responsible for certificate and certificate status
  - Issuance
  - Revocation
  - Overall management
- Always includes a Certification Authority (CA)
- May include
  - Registration Authorities (RAs)
  - Other subcomponents

Certificate Issuing and Management Component (CIMC)

- Consists of:
  - Hardware, software, and firmware responsible for performing CIMS functions
- Does not include:
  - Environmental controls (e.g., controlled access facility, temperature)
  - Policies and procedures
  - Personnel controls (e.g., background checks and security clearances)
  - Other administrative controls

CIMC Protection Profile (PP)

- Develop a protection profile to be validated as part of the National Information Assurance Partnership (NIAP)
  - Goal: enable validation of essential security requirements of the certificate issuing and management part of a PKI product
- Specify complete set of functional and assurance security requirements

CIMC PP (concluded)

- Specify all the *mandatory* technical features of a CIMC
  - Independent of the subcomponent performing the function
  - Must implement all security requirements for all mandatory functions
- Specify requirements for *optional* technical features
  - Must implement all security requirements for incorporated optional functions

CIMC PP Development Process

- Initial version developed with English language requirements text
  - Requirements developed in cooperation with research partners
    - Aided in document review and ensuring completeness
  - Includes four increasing levels of security
  - Consistent with FIPS 140-1 security requirements

CIMC PP Development Process (concluded)

- Document conversion to protection profile (PP) underway
- Each draft publicly available for comment

CIMC PP

- Comments and recommendations...

Contacts

- Current version of the document is available at:

http://csrc.nist.gov/pki/documents/

Contacts:

annabelle.lee@nist.gov

david.cooper@nist.gov

kathy.lyons-burke@nist.gov